



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/529,353	03/25/2005	Martin C Rosner	US020357US	2542
24737 7590 10/20/2009 PHILIPS INTELLECTUAL PROPERTY & STANDARDS P.O. BOX 3001 BRIARCLIFF MANOR, NY 10510				
EXAMINER				
OKEKE, EZUNNA				
ART UNIT		PAPER NUMBER		
2432				
MAIL DATE		DELIVERY MODE		
10/20/2009		PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/529,353

Applicant(s)

ROSNER ET AL.

Examiner

IZUNNA OKEKE

Art Unit

2432

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 29 June 2009.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-28 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-28 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SF/ICE)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed 06/29/2009 have been fully considered but they are not persuasive.

On pages 1 and 2 of applicant's argument, applicant argues that Lundkvist fails to anticipate the limitation in claim 1 of "communicating a first response from the target node to the source node, immediately after the query is received and before the query is decrypted at the target node".

Applicant argues that the signal 'Z' in Lundkvist is sent after the signal 'X' is decrypted.

Applicant cited the box in fig. 3 to back up the argument. Applicant further argues that Lundkvist cannot transmit a response 'Z' before the message is decrypted because the identity information unique to the object is encrypted in the message 'X'.

Applicant's amendment and argument does not overcome the rejection because Lundkvist teaches the applicant's invention. For the purpose of clarification, reproduced below are the elements in Lundkvist's invention and how they relate to applicant's invention.

The Object 1 in Lundkvist can be equated to the applicant's source node.

The Portable Unit 2 in Lundkvist can be equated to the applicant's target node.

The signal X in Lundkvist can be equated to the applicant's query.

The first response (Z) can be equated to the applicant's response 1.

The second response (Y2) can be equated to the applicant's response 2.

According to applicant's specification in Para 11, the first response is used in measuring the proximity of the nodes by calculating a time duration between the transmission of the query and the receipt of the first response. The second response is used in verifying the authenticity of the

target node. Lundkvist discloses a similar invention. In Para 34, when the Object 1 sends the signal 'X' to the portable unit, a first response 'Z' is sent to the Object 1, the first response comprises a random number and an identity of the Portable Unit 2 or target (and not that of the Object 1 or source as applicant stated... See Para 34, Lines 6-7). The decryption of the signal 'X' has nothing to do with the transmission of the first response 'Z'. The box in fig. 3 which applicant alludes to is for illustration purposes and doesn't teach that the decryption of 'X' is instrumental to the transmission of the first response 'Z'. The decryption of the signal 'X' only affects the second response Y2 (as the response comprises $f(x)$) but the first response 'Z' is transmitted once 'X' is received. In fact, in Para 34, Lines 1-3, Lundkvist teaches that 2 signals (Z and Y2) are sent in response to 'X'. The first signal 'Z' (used for measuring proximity) is sent once 'X' is received and the second signal 'Y2' (used for authentication) is sent at a later time using decrypted information from 'X'.

This is clearly stated in Para 34, after 'X' is decrypted then the second response 'Y2' is calculated from the decrypted 'X'. In Para 34, the second response 'Y2', comprises a first part $f(x)$ (a function of the decrypted signal 'X') and a second part $f(z)$ (a function of the first signal which is used for verifying the authenticity of the unit). The Object 1 or source measures a time from the transmission of the 'X' to receiving the first response 'Z' and then authenticates the unit using the received second signal 'Y2'. So, the processing or decrypting of the signal or query 'X' has nothing to do with transmission of the first response 'Z' by the portable unit and as clearly stated by Lundkvist, this first response is used in determining the proximity from a measured time value. It will also defeat the purpose Lundkvist's invention (determining proximity) if the 'X' query is first decrypted or processed (and a value from the signal used in the generation and

transmission of 'Z') before the first signal 'Z' is transmitted because proximity determination entails sending a query and receiving a response immediately to measure the elapsed time and determine the proximity of the object.

In view of the above explanations, examiner maintains the rejection because applicant's argument does not make the invention wholly and patentably distinct from the prior art disclosed by Lundkvist.

Double Patenting

2. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

3. Claims 1-28 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-21 of copending Application No. 10529778. Although the conflicting claims are not identical, they are not patentably distinct from each other because both invention and claims are directed to a method of determining the

proximity of a target node to a source node by communicating a query to one node and receiving a response.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 102

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action

1. Claims 1-7, 11-25 are rejected under 35 U.S.C. 102(e) as being anticipated by Lundkvist (US-2003/0184431).

a. Referring to claim 1, 11 and 18:

Regarding claim 1 and similar claims 11 and 18, Lundkvist teaches a method of determining proximity of a target node to a source node, comprising:
communicating a query from the source node to the target node; communicating a first response from the target node to the source node, immediately after the query is received and before the query is decrypted at the target node; receiving the first response at the source node (See the response to argument and Para 34 teaches communicating a query (X signal) from a source node to a target node and communicating a first response (Z signal) from the target node to the source node and receiving the Z signal response at the source node);
processing the query at the target node to produce there from a second response that facilitates a verification of the target node and its first response; communicating the second response from the target node to the source node (Para 34 teaches processing the signal to produce a second response (Y2 signal which is function of the query and the first response) which is sent to the

source node);

determining a measure of communication time between communicating the query and receiving the first response; and determining the proximity of the target node based on the measure of communication time (Para 34 teaches a time T2 which is measured from the transmission of the query (X signal) to the reception of the first response (Z signal) wherein the proximity of the target node is determined based on comparing the time T2 to a predetermined value).

a. Referring to claim 2, 12 and 19:

Regarding claim 2 and similar claims 12 and 19, Lundkvist teaches the method of claim 1, wherein the query and at least one of the first and second responses correspond to at least a portion of a cryptographic key-exchange protocol (Para 29 and 34 teaches the signals corresponding to a cryptographic key-exchange protocol such as asymmetric key pair cryptography).

a. Referring to claim 3, 13 and 20:

Regarding claim 3 and similar claims 13 and 20, Lundkvist teaches the method of claim 2, wherein the key-exchange protocol corresponds to a Needham-Schroeder key-exchange protocol (Para 29, Line 12-14 teaches a symmetric key encryption which is a type of Needham-Schroeder protocol can be used in the key exchange).

a. Referring to claim 4, 14 and 21:

Regarding claim 4 and similar claims 14 and 21, Lundkvist teaches the method of claim 1, wherein the query and at least one of the first and second responses correspond to at least a portion of an OCPS protocol (Para 29 and 34 teaches the first and second response

corresponding to an authentication stage, a key exchange stage, a key generation phase and a data transmission phase of the OCPS protocol).

a. Referring to claims 5, 15 and 22:

Regarding claim 5 and similar claims 15 and 22, Lundkvist teaches the method of claim 1, wherein the query includes an encryption of an item based on a public key of the target node (Para 29 and Para 31 teaches the encrypting identity information and the random number based on asymmetric key pair cryptography such as the public key of the target node), and the processing of the query includes decrypting the item based on a private key of the target node, for inclusion in the second response (Para 29 and Para 34 teaches the portable unit decrypting the item based on asymmetric key pair cryptography).

a. Referring to claim 6, 16 and 23:

Regarding claim 6 and similar claims 16 and 23, Lundkvist teaches the method of claim 5, wherein the first response includes a random number, and the processing of the query further includes encrypting the item and the random number using a public key of the source node to form at least a portion of the second response (Para 34, teaches the first response which includes a random number and Para 29 teaches encryption of all responses sent between the nodes. Para 34 the second response Y2 being a function of the first response which includes the random number and the object ID).

a. Referring to claims 7, 17 and 25:

Regarding claim 7 and similar claims 17 and 25, Lundkvist teaches the method of claim 5, wherein the first response includes an encryption of a random number based on a public key of

the source node (Para 34, teaches the first response Z as an encrypted signal comprising the first information which consists of a random number).

a. Referring to claim 24:

Regarding claim 24, Lundkvist teaches the node of claim 23, wherein the second response further includes a signature of the decryption of the item and the random number, using a private key of the target node (Para 34 teaches a second response Y2 which includes an encryption of a random number based on a public key of the node).

Claim Rejections - 35 USC § 103

2. Claims 8-10, 26-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lundkvist (US-20030184431), and further in view of Davis et al. (US-6088450).

a. Referring to claims 8 and 26:

Regarding claim 8 and similar claim 26, Lundkvist teaches the method of claim 1, wherein determining the proximity includes comparing the communication time to a threshold value.

Lundkvist does not teach distinguishing between local and remote nodes based on the proximity.

However, Davis teaches distinguishing between local and remote nodes based on the proximity (See Davis, Col 4, Line 2-11 teaches distinguishing between local and remote nodes by determining when a device is within the proximity level).

Therefore, it would have been obvious to one of ordinary skill at the time the invention was made to modify Lundkvist's system to be used in a network to determine local and remote nodes as taught by Davis for the purpose of providing security for the network by allowing

access to resources within a specified boundary and limiting access to sources outside the boundary

a. Referring to claims 9 and 27:

Regarding claim 9 and similar claim 27, the combination of Lundkvist and Davis teaches the method of claim 1, further including restricting communications with the target node based on the proximity (See Davis, Col 4, Line 2-11 teaches prohibiting communications with nodes outside of the proximity perimeter).

a. Referring to claims 10 and 28:

Regarding claim 10 and similar claim 28, the combination of Lundkvist and Davis teaches the method of claim 1, further including restricting access of the target node to system resources based on the proximity (See Davis, Col 4, Line 2-11 teaches prohibiting access to resources from nodes outside of the proximity perimeter).

Conclusion

3. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to IZUNNA OKEKE whose telephone number is (571)270-3854. The examiner can normally be reached on 9:00am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/I. O./
Examiner, Art Unit 2432

/Jung Kim/
Primary Examiner, AU 2432